FORTINET
High Performance Network Security

FortiAuthenticator Agent for Microsoft IIS/OWA - Install Guide

REVISION 1

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

06/10/2015

FortiAuthenticator Agent for Microsoft IIS/OWA - Install Guide

Revision 1

TABLE OF CONTENTS

Change Log

Date	Change Description
2015-01-19	Initial release.

Introduction

This document introduces FortiAuthenticator Agent for Microsoft IIS, a plugin for the Microsoft IIS web server which allows a FortiAuthenticator OTP requested during web server authentication, including during Microsoft Outlook Web Access authentication.

This document also covers the installation and configuration of the FortiAuthenticator Agent on supported Microsoft Windows Server, IIS, and Exchange systems, and configuration of the FortiAuthenticator.

FortiAuthenticator Agent for Microsoft Windows

Once installed, the modified login process requires a Username and OTP (One Time Passcode) to be validated via the FortiAuthenticator, and the Username and Password validated as normal via AD (Active Directory).

FortiAuthenticator Agent validates the OTP prior to the AD password which prevents any possibility of brute forcing the password.

Due to the fact that the username, password, and token need to be simultaneously put into the login prompts, two-factor authentication methods that require a trigger to obtain the token (email and SMS) are not supported. However, other methods including FortiToken and FortiToken Mobile are supported.

Supported Software Versions

This install guide is based on FortiAuthenticator Agent for Microsoft IIS v.1.0.0 which has been tested with:

Operating Systems

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2008 R2

Applications

- Microsoft IIS 7.0 and later
- Microsoft Exchange Server 2010 & 2013

System Requirements

FortiAuthenticator Agent for Microsoft IIS v.1.0.0 has the following system requirements:

- 20 MB of free disk space
- TCP/IP networking
- Microsoft .NET Framework 4 Client Profile or later
- Visual Studio C++ 2012 redistributable packages

FortiAuthenticator Agent for Microsoft IIS v.1.0.0 currently does not test for the IIS/Exchange presence or for the appropriate .NET runtime versions. This will be resolved in a future revision.

Required Ports

The following ports must be allowed between the Client operating system and the specified system:

Port	Destination	Description
TCP/443	FortiAuthenticator	Used by the FortiAuthenticator Agent for Microsoft Windows to validate the entered Two-Factor Authentication Token.
TCP/389	Windows Domain Controller	Indirectly used by the FortiAuthenticator Agent for Microsoft Windows to verify group membership of the user in order to identify if Two-Factor Authentication should be applied.

Third Party Trademark Notice

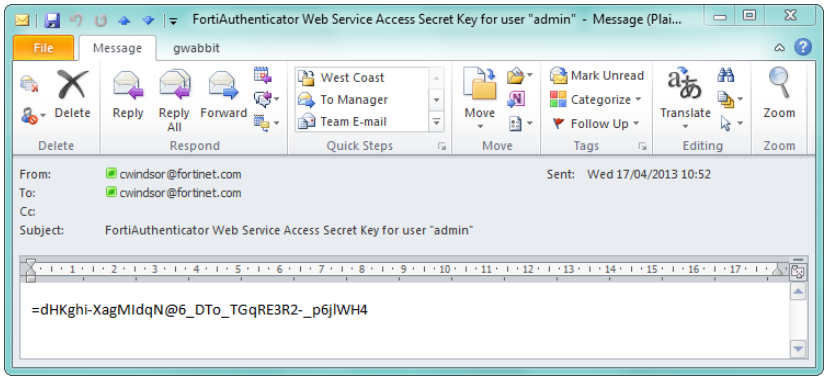
Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

FortiAuthenticator Configuration

To enhance the Microsoft Windows operating system login with the use of a OTP (i.e. the two-factor authentication token), FortiAuthenticator Agent for IIS (including OWA) uses the FortiAuthenticator REST API. To use the REST API, a key is required which must be generated before installing the desktop agent software.

Generating an API key requires a working email configuration. Before proceeding, configure and test an email server in *System* > *Messages* > *SMTP Servers* and set it as active in *System* > *Messages* > *Email Services*.

1. Log into the FortiAuthenticator.
2. Edit the admin user in *Authentication* > *Local User Management* > *Local Users* and enable *Web Service Access* in the *Role* section. Click *OK* and an email containing the API Key for that user will be sent.



The required users should be imported via LDAP and assigned a FortiToken with which to authenticate before proceeding.

Agent Installation Procedure

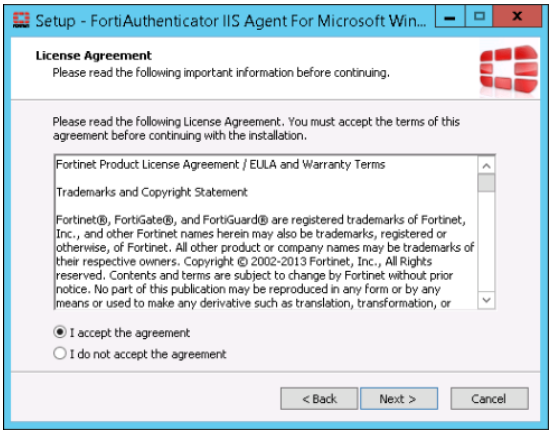
Before proceeding, please backup your system and all configurations files.

FortiAuthenticator Agent for Microsoft IIS is designed for installation onto a Domain connected system. On the IIS/OWA system you wish to perform two-factor enhanced login:

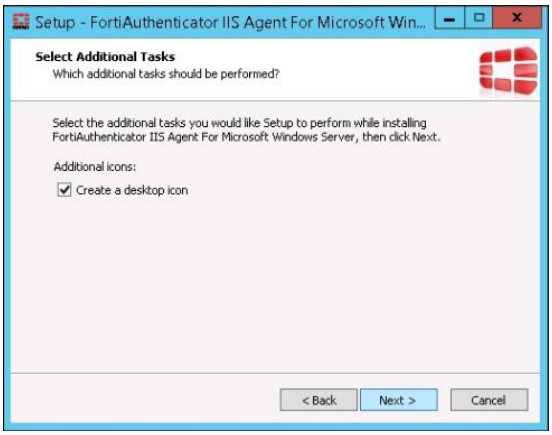
1. Ensure your system meets the pre-requisites as defined in System Requirements.
2. Run the FortiAuthenticator Agent install file as a Domain Administrator (e.g. either as a logged in Domain Administrator or by right-clicking and select *Run as Administrator*. Note that the Agent can also be installed via GPO, however that process is not covered in this document.

   FortiAuthenticator Agent for Microsoft Windows will now begin to install.

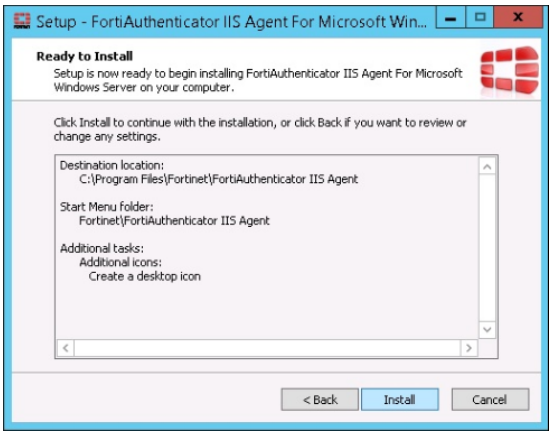
3. Select *Next* to continue with the installation.



4. Read and accept the *License Agreement*, and click *Next*.



5. Select *Create a desktop icon* if you wish to access the Agent via the desktop.



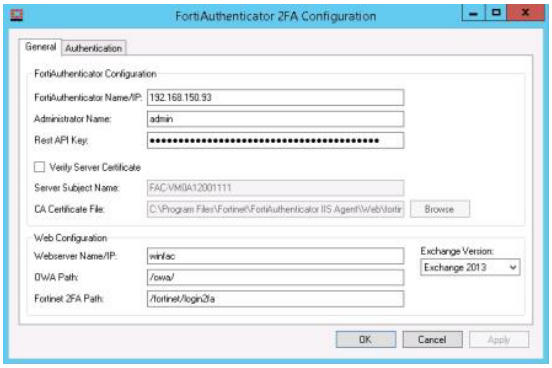
6. Click *Install* to begin the installation process.

Once the installation has completed, tick *Review 2FA Configuration* and click *Finish*.

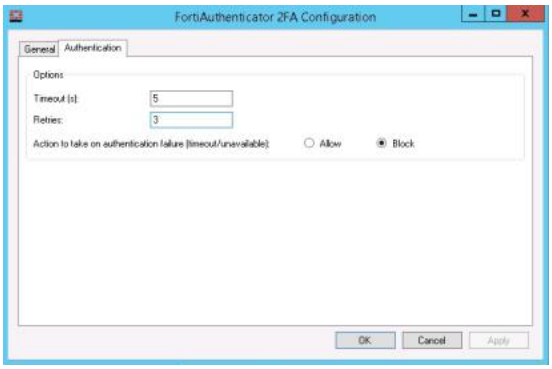
The configuration dialogue should open. If it does not, or if you wish to reconfigure your agent, run the FortiAuthenticator Agent for Microsoft IIS configuration utility to configure the specifics of your setup.

Agent Configuration

1. When the FortiAuthenticator Agent for Microsoft IIS configuration utility opens, click the *General* tab.



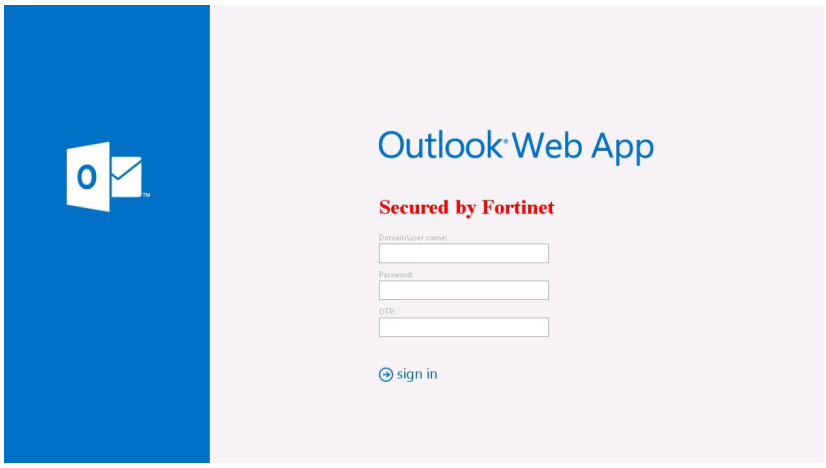
2. In the *FortiAuthenticator 2FA Configuration* screen, configure the IP address, username, and API key obtained in *FortiAuthenticator Configuration*.
3. In the Web Configuration section, configure the specifics of your Web Server and OWA installation.



4. Select the *Authentication* tab and configure the required timeout and retry parameters, as well as the action to take should the FortiAuthenticator become unavailable (*Allow* or *Block*). Click *OK* to save.

User Two-Factor Login

The default installation creates a modified version of the OWA login page as shown below which is enhanced with an OTP login dialogue. Users should enter their username and password as usual but add the OTP code from their FortiToken or FortiToken Mobile as the second factor.



This template can be modified by editing the webpage CSS/JS if required.

While this plugin protects Microsoft IIS with Outlook Web Access, two-factor authentication will not be applied to other protocols such as POP3/IMAP traffic.

Appendix A — Licenses

FortiAuthenticator utilizes elements of Open Source technology including:

pGina - http://pgina.org/

License for use of such software is reproduced below as per the terms of use.

pGina License

Copyright (c) 2013, pGina Team

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the pGina Team nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright© 2015 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations,and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.